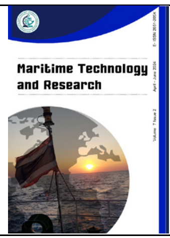
Maritime Technology and Research

https://so04.tci-thaijo.org/index.php/MTR




Review Article

# Literature review of maritime cyber security: The first decade

**Avanthika Vineetha Harish, Kimberly Tam[*] and Kevin Jones**

*University of Plymouth, Drake Circus, Plymouth PL4 8AA, United Kingdom*

[*]*Corresponding author's e-mail address: kimberly.tam@plymouth.ac.uk*

**Article information**
Received: July 11, 2024
Revision: October 1, 2024
Accepted: October 8, 2024

**Keywords**
Comprehensive review;
Maritime cyber security;
Cyber-physical security

**Abstract**
This is a comprehensive review of the current body of work for cyber security in the marine and maritime sectors. Reviews are useful as a field develops, both for those new to the field, and those contributing to a section of the existing body of work. This looks at the phases of research, from exploratory and positional papers in the early 2010s, to the more recent experimental research, and how "maritime cyber security" has branched into subtopics addressing human factors, policy, law, cyber-physical security, and more. In addition to different topics of research, this comprehensive review summaries the focus of those papers, whether they are intended for crewed vessels, uncrewed vessels (above and below the surface), offshore structures (e.g., oil, renewable wind energy), and infrastructure like ports. As a newly developing field, compared to general cyber security or naval engineering, this review also examines the ratio of positional papers, papers that generate knowledge, and papers that summarize existing works to gauge the maturity of the field. This type of review relies on an expert understanding of the existing body of academic literature and its impact on industry and government, instead of applying prescribed systematic review methodology. This review of over three hundred articles concludes with overall findings and suggestions for future research to continue maturing and growing maritime cyber security research.

## 1. Introduction

According to Google trends[1], the first mention of "maritime cyber security" ("maritime cybersecurity" was introduced a few years later), was first searched for in December 2013 (see **Figure 1**). Some of the earliest and most recognized academic papers were also published in 2013. Several of these earlier publications were positional papers, articles that began to describe the potential issues around cyber security of ocean-related technologies. Interest in the subject noticeably increased in 2016, and significantly again in 2020. In an examination of 319 maritime cyber security papers from 2013 - 2023, the first review articles in the field were published in 2017, which is early, considering that there were only 15 - 20 maritime cyber security papers available for review around that time. In the analysis, later review studies had had access to more articles, but had selected a small subset for review. In contrast, this comprehensive review provides a high-level analysis of the first decade of research without exclusion, and an in-depth review of key works to establish the breadth, depth, and maturity of the body of research.

[1]https://trends.google.com/trends

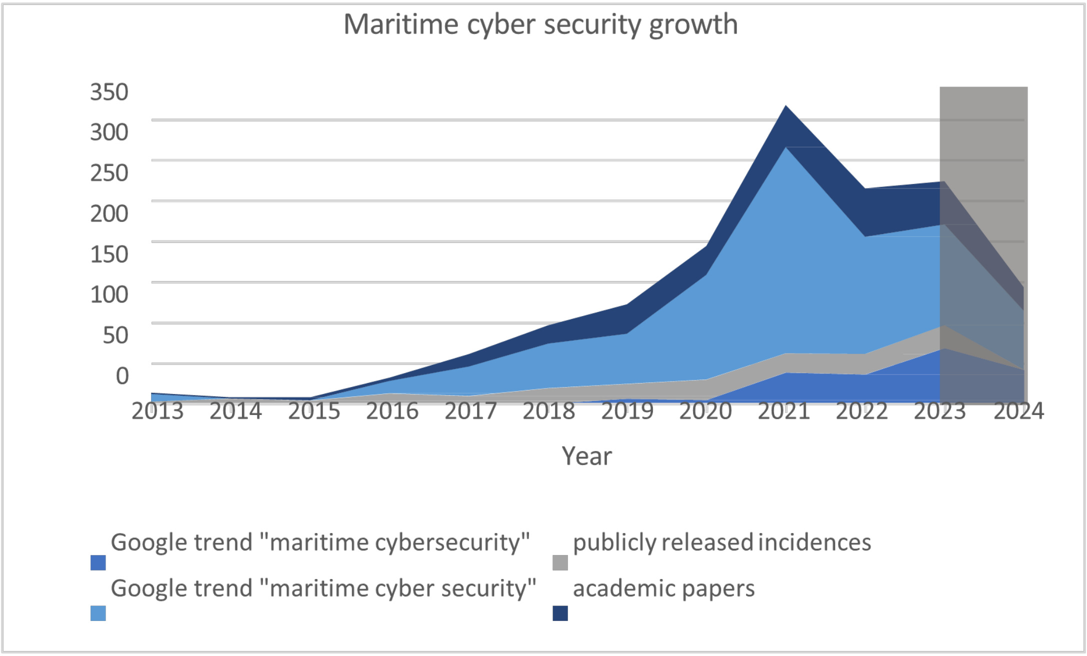



**Figure 1** Global public Google search trends[1] for two terms, number of academic papers, and public incidences (Fenton, 2024) from the start of 2013 to mid-2024.

### 1.1 Cyber threat impact on the industry

As a billion-dollar industry, the maritime sector facilitates international trade and interconnects the world. In 2022, a total of 11 billion tons of goods were transported by ships, including 3 billion tons of crude oil and 3.3 billion tons of iron ore (UNCTAD, 2022). Maritime infrastructure, which includes ships, port infrastructure, and offshore structures, is an essential part of the modern world and its economic growth.

The traditional concept that maritime systems are air-gapped from land or the wider world is no longer true, across both operational and information technology (OT and IT). New technologies are becoming more networked, resulting in better communications, usability, and service, but they also introduce vulnerabilities when not secured appropriately. A 2021 US Coast Guard report claimed the number of reported cyber attacks against maritime transportation systems had increased by 68 % since 2020 (US Coast Guard, 2022). **Figure 1** combines Google search trends, public incident statistics from the Maritime Cyber Attack Database (MCAD) from Fenton (2024), and academic publications to show the overall growth in interest (public and academic) over the decade from 2013 - 2023, with the addition of incomplete 2024 statistics.

Cyber security for Critical National Infrastructure (CNI) gained huge attention after the 2010 Stuxnet attack, which targeted supervisory control and data acquisition systems (SCADA). More recently, in 2017, the NotPetya Malware was used in a global cyber attack, affecting systems worldwide. The global shipping giant Maersk shipping line was significantly impacted by this attack. According to Maersk, who have been congratulated on their response and transparency, they suffered losses of between 250 - 300 million USD revenue losses, IT restoration costs, and extraordinary operations costs (A.P. Moller - Maersk, 2017). This is not an isolated event, as denial of service and ransomware are the most frequently, publicly, reported attacks. However, there may be some bias, as “publicly” reported attacks such as these are easier to see and report than attacks that manipulate data stealthily, like Stuxnet. While this is understandable, studies based only on public information should be open about this bias for readers. In 2022, German oil companies Oil Tanking and Mabanaft suffered an attack, which was thought to be a ransomware attack, that caused huge distress to its loading and unloading systems, forcing the energy company Shell to reroute supplies to other depots (Greig, 2022). In the year prior, news of attackers threatening to publish data stolen from the website and servers of the Port of Lisbon was made (Rahman, 2023). An attack on DNV's ShipManager servers affected more than a thousand ships worldwide (Page, 2023); attacks on Dutch maritime logistics company Royal Dirkzwager released potentially stolen data (Arghire, 2023), and attacks on Japan's port of Nagoya caused it to momentarily suspend their container operations (Robinson, 2023).

Denial of service (DoS) attacks have also been reported. The online website infrastructure of the Port of London Authority was knocked offline by a 'politically motivated' Distributed DoS (DDoS) attack in 2022 (Glover, 2022), while later that year, the inspection database of the Tokyo MOU, which coordinates port state control across the Pacific region, was attacked and taken down for several weeks (Maritime Executive, 2023). In another incident, Voyager Worldwide, a vessel management software and navigation services provider, took all of their systems offline (Chambers, 2022). Port DoS attacks in 2023 include two Israeli ports' websites (Haifa Port and the Israel Ports Development and Assets Company The Times of Israel, (2023)), the websites of three Canadian ports (Quebec City, Halifax, Montreal (Morrissette-Beaulieu, 2023)), the North Sea Port website that operates the ports of Vlissingen, Terneuzen and Ghent (Harreveld, 2023), and the websites of the Dutch port authorities of Groningen, Amsterdam, Rotterdam, and Den Helder (NL Times, 2023).

Earlier positional papers such as Jones et al. (2015), ESC Global Security (2015), Tam and Jones (2018) hypothesized that cyber attacks, such as denial of service and ransomware in the maritime sector, could have an impact on physical operations and increase risks to safety, and these public 2020s incidences verified those predictions. Cyber attacks against the sector are motivated by a variety of reasons, such as egoism, espionage, financial gain, and political agendas Silgado (2018). According to the US Coast Guard (2024), ransomware attacks increased by a further 68 % between 2022 and 2023, on top of the significant increase the year before (US Coast Guard, 2022). Many of these reports were also about DoS or ransomware. From these known incidences, and others, it is clear that the impact of disrupting the maritime operation is not confined to the sector itself, but also impacts sectors and industries dependent on it, such as food supply, electronic manufacturing, oil and gas, and the wider supply chain.

In response to growing cyber security concerns, the International Maritime Organization (IMO) passed Resolution MSC.428(98) to raise awareness about cyber risk threats and vulnerabilities. As of January 1st, 2021, all ship owners must comply with this resolution to continue their operations around the world (International Maritime Organization, 2017). Other documents that considered this problem include IMO's circular MSC-FAL.1/Circ.3 for guidelines on maritime cyber risk management, and Baltic and International Maritime Council's (BIMCO) cyber security for on-board maritime vessels document (International Maritime Organization, 2022; BIMCO, 2021). These documents emphasize the importance of identifying vulnerabilities in ship systems, as well as installing countermeasures for cyber attacks (BIMCO, 2021).

It is important to continue supporting the cyber security and resilience of the sector with scientific findings that can also be fed into new solutions, policies, training, and governance. To do so, research publications require academic rigor both in individual publications and in the larger body of work, which this review attempts to assess.

### 1.2 Review structure

The aim of this comprehensive review is to examine the last decade of academic research on the topic of maritime cyber security. In the review of the literature, the first paper that examined maritime cyber security as one topic, and not as a piece of a larger topic, was in 2013. The time frame for this review is, therefore the complete years from 2013 - 2023, but also partial statistics from 2024, due to the time of publication.

A wide range of papers has been considered by the authors. Generally, the mass majority of literature found were predominately conference papers, journal papers, and theses. This comprehensive review includes of all these types of publications because, at the start of a field, many key journals and conferences will not accept positional papers or new topics which are not in their accepted topics list.

Because of this, many previous survey papers missed high impact publications by limiting themselves to specific journals and conferences. In contrast, this review has also considered articles published in many languages, although non-English publications were translated to English using Google translate.

There are two parts to this review. The first is to select key papers in specific topics to illustrate how maritime cyber security has branched out into subtopics. The second part of this review looks at 300+ papers from January 2013 - June 2024, published in a range of venues and languages, to examine the maturity of the field after its “first decade” in existence. To do this, papers are divided into three main categories:

1) Positional: These articles often propose an area of research, or state an issue with greater clarification than before. Some of these will also propose a type of solution, but not in detail, nor would they implement or test the solution.

2) New knowledge: These papers add new knowledge to the body of knowledge. This can be further broken up into papers based on experiments and ones that propose new solutions (e.g., frameworks, simulations, testbeds) with more depth and verification than positional papers. In theory, in this category papers that generate new knowledge by surveying or interviewing a wide range of experts are considered. However, as most interview/questionnaire studies examined lacked rigor (very few participants, or did not fully disclose/verify the background of experts or methodology), the majority of these studies are classified as a review of people’s opinions, instead of generating new knowledge.

3) Surveys: Literature reviews, including systematic reviews, are included in this category. This includes reviews made by surveying experts, instead of surveying papers, and combining expert opinions with existing frameworks.

These categories are subjective, with some papers borderline between categories. Others, particularly theses, contain enough material that multiple sections covered multiple categories. In these cases (0.5 % of all papers), some articles have two classifications. Using the definitions above, 319 papers are divided into four categories to assess the growth of research, from positional papers to papers that create new knowledge, and then papers that summarize and contextualize that knowledge. All papers were found by searching google scholar, scopus, and ACM using “maritime cyber security” “maritime cybersecurity” and “maritime cyber-security”. While it is recognized this may not cover some papers peripheral to the subject, there is high confidence that the sample pool is larger than previous studies, and includes the most field defining and significant papers in the first decade of this field. **Figure 2** shows the distribution of these papers and also which of them correspond to Sections 2 - 5 of this article. The overall analysis of all papers is then explored in the Discussions (see Section 6) after reviewing key papers in the field and of these categories.

In-depth analysis of sector-specific equipment is not the focus of this paper, but a few key systems that appear frequently in the literature are the Automatic Identification System (AIS), Integrated Bridge System (IBS), Integrated Navigation System (INS), Voyage Data Recorder (VDR), Human Machine Interface (HMI), Program Logic Controllers (PLCs), and controls for rudder, thrust.

## 2. Positional papers

As a new area of research, there has been a steady number of positional papers from 2013 - 2024 as new subtopics were explored, as shown in **Figure 2**. Examining positional papers, often the first to detail a new subtopic, is a useful way to understand how the topic of “maritime cyber security” has branched off into new topics. Typically, when examining the literature over the last decade, new subtopics of the umbrella term maritime cyber security began with a positional paper. That said, not all positional papers proposed new subtopics.

In the analysis of the literature, many of the more recent positional papers were for specific nations or sea regions. This highlights that, while this is a global issue, there are unique challenges for different nations, sea regions, ports, ships, and organizations. For example, the very first positional paper in 2013 was specific to the United States (US). Key positional papers for Australia, South Africa, Greece, Korea, Portugal, Spain, France, the United Kingdom, Norway, Indonesia, Bangladesh, Vietnam, and the Philippines were seen up to 2023. Some also focused on Navy challenges specific to countries over the merchant navy. Many positional papers also focused on sea areas, such as the Black Sea and the Malacca straits, due to local threats.

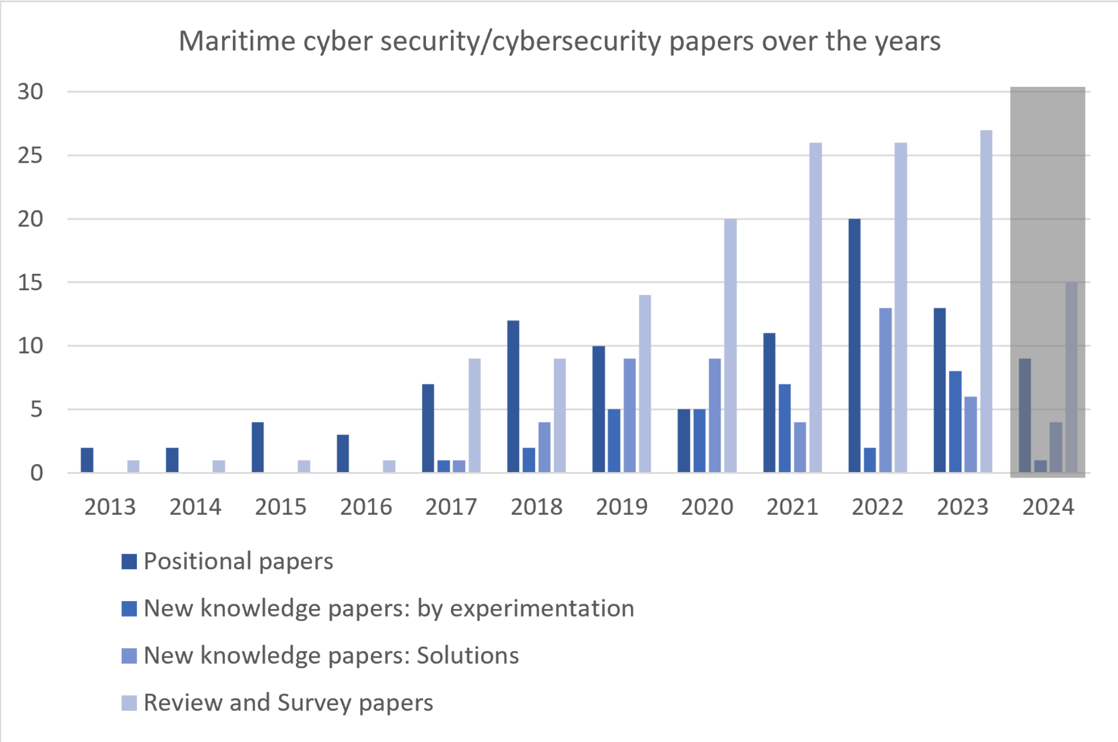



**Figure 2** Proportion of types of papers and relevant sections.

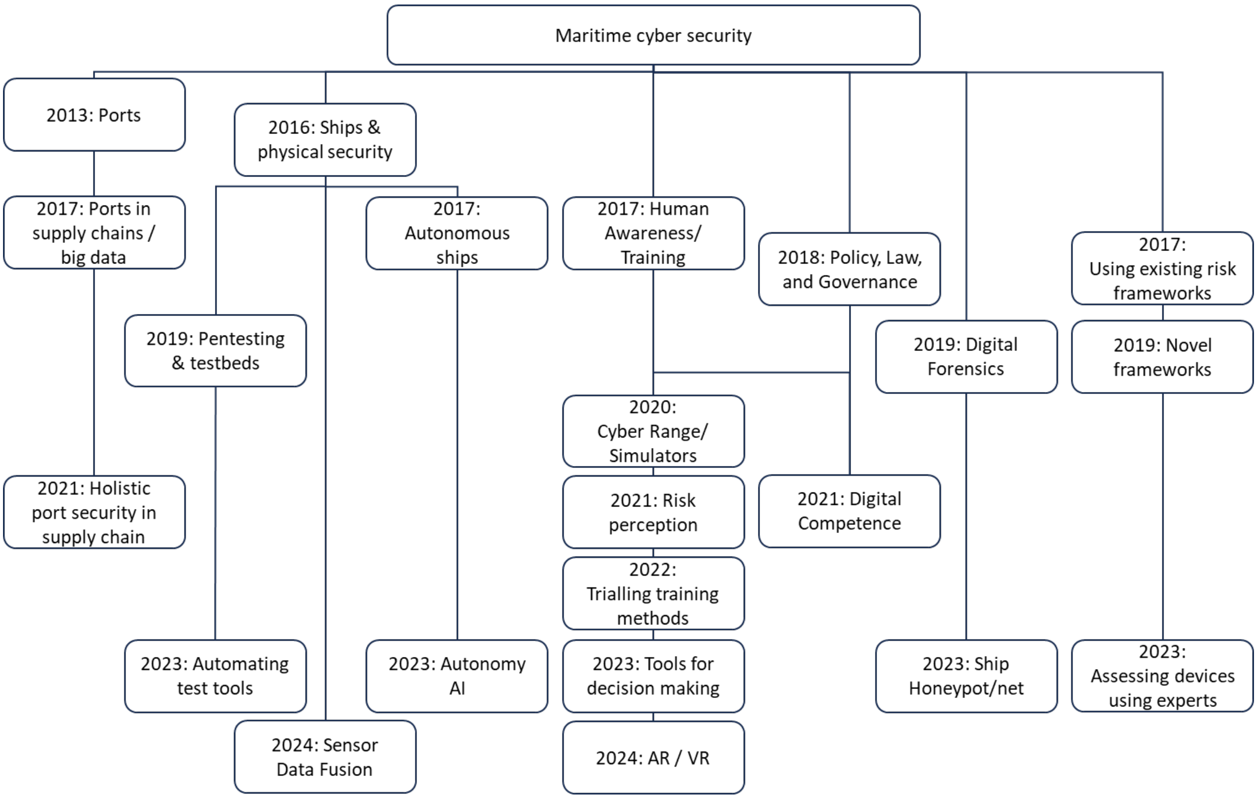



**Figure 3** Tree of positional papers and new topics of study.

Before 2019, the majority of publications were in the early phase of predominantly positional papers (everything before 2017 was either positional or review). However, from 2019 until 2024, the number of survey papers has outnumbered positional papers. This raises concerns whether the body of research is more forward facing (positional) or backwards facing (review), which is discussed at the end of this paper. While the number of positional papers outnumbered the two new knowledge categories separately most years (the exception being 2020), when compared to the two new knowledge categories combined, they outnumbered positional papers in 2019, 2021, and 2023.

To better understand how the topics of maritime cyber security have grown in breadth and depth, **Figure 3** shows positional papers 2013 - 2024 based on topics. From these articles, it is possible to look at when topics first began to emerge globally. This does exclude positional papers that are a variation of a global idea; for example, while maritime cyber security policy was first discussed in 2018, and is mentioned here, there have been many papers on policy for specific regions like the Philippines, which is not shown on this graph. From the analysis, "maritime cyber security" was split into port and ship cyber security early in the field's development, between 2013 - 2016. 2016 also saw more discussion on OT security in addition to IT security. The research of "ships" was also split fairly early in 2017 to crewed and different levels of autonomous vessels. While there have been some efforts to consider the holistic security of ports and ships together in Tam et al. (2021a), most articles addressed just one.

The human element of maritime cyber security has generated many topics since the first positional papers appeared around 2017. After a few years of discussions around the need for awareness and training, 2020 saw the first positional papers on teaching facilities like cyber ranges (CRs) and crew training simulators that can be adapted for maritime cyber security training. This was quickly followed by positional papers on how people in the sector perceived risk and trialing actual training sessions using cyber ranges, tabletops, and ship simulators. With a better understanding of the problem, 2023 and 2024 saw new positional papers on creating tools to aid human-made decisions and discussions on how to use more future digital technologies to improve training and cyber security awareness. In 2021, there was a cross between policy and the human element, when the discussion of digital competence was first discussed. Papers on cyber security codes and maritime law had their clearest beginnings in 2018, such as with Hopcraft and Martin (2018). Since then, there have been a few papers that looked into the legal aspects of maritime cyber security and IMO regulations (Al Ali et al., 2021; Karim, 2022). The majority of papers in the period 2018 - 2023 summarized the current state of affairs, and clear branches of subtopics prior to 2024 were not seen by the authors of this paper.

Lastly, there is an area of work focused on capturing malicious behaviors (digital forensics, and tools to collect like honeypots), which started in 2019 but compared to other areas has not received much attention. This is also somewhat connected to risk assessment frameworks, which started in 2017 using existing frameworks to assess risk and some discussion on how to create novel frameworks in 2019. Since then, other frameworks like MITRE have been adapted for the sector and/or used to assess specific devices using expert opinions as input.

From **Figure 3**, it is possible to understand the growth of the body of work, and even make educated predictions on future areas of work (see Section 6). As the field continues to develop and mature, the number of positional papers has decreased proportionally to other types of papers, and this trend is likely to continue; however, for the field to grow, a few key positional papers every few years is key for the next decade or two, to expand on topics of research individually and through cross-topics as well.

## 3. New knowledge papers: by experimentation

This section focuses primarily on papers that generate new knowledge through experiments, as defined in Section 1. New knowledge papers that discuss solutions that are at least one step above a proposal follows this section. As surveys combine and comment on these types of papers, they are discussed last. Within this section, different types of experimental papers are discussed by their type, scope, and setups. Topics that are more positional for future work are not included in this section.

### 3.1 Types of assessments

In this paper's review of past literature, most assessments made tended to be technical vulnerability assessments. While training solutions have been published for people (see Section 4.4) there is a gap in the research that evaluates these training solutions and learning. Similarly, most papers on policy/standards seem to be primarily positional statements. The one exception to this seen was an experiment assessing how well standards compliance actually provided digital security (Hopcraft et al., 2023).

A vulnerability assessment identifies digital flaws, often reporting them with risk scores or mitigation steps. Some already-existing vulnerability scanning tools have revealed more than 50,000 external and/or internal weaknesses in systems (Spivey, 2021). The purpose of a penetration test (pentest) is to then exploit these vulnerabilities as an attacker would, and report the results. The UK National Cyber Security Centre (NCSC) recommends a well-scoped penetration test as a method of system hardening against threats (NCSC, 2022). For the interested reader, details on security audits, vulnerability assessments, and ethical hacking are differentiated in Chia (2019). This positional paper proposes the necessity of ethical hacking in the marine and maritime sectors, and urges shipping companies to deploy tests to check their cyber resilience. Another type of assessment is a security audit, which determines if policies and procedures are compliant with standards and regulations.

For IT systems, there are several vulnerability assessment and penetration testing frameworks, but as of publication, there are very few established tools for the maritime industry, particularly the OT side of the sector. In a systematic literature review by Bolbot et al. (2022), out of the 144 papers examined from 2010 - 2022, only thirteen papers were attributed to penetration testing and vulnerability scanning. This more limited systematic review claimed that the majority of testing focused primarily on IT testing, and not OT. These findings were confirmed in the current paper's wider comprehensive analysis of existing literature on vulnerability assessments.

Penetration tests of an off-the-shelf satellite communication device using commonly available tools and custom scripts were done in Gurren at al. (2023). These tests also demonstrated side effects, such as extreme battery drainage. This was one of the few experimental papers that demonstrated the possible cyber-physical effects of a device. In Pavur et al. (2020),, four major Very Small Aperture Terminals (VSAT) networks were tested, all of which used the same underlying technology stack used by more than 60 % of the world's maritime industry. These streams were found to lack basic link-layer encryption, and were susceptible to passive and active attacks such as eavesdropping and session hijacking, which exposed ship-to-shore communication to cyber risks.

Tests were also conducted on the security of Voyage Data Recorders (VDR), a system that stored evidence for incident investigations, by testing them for known and unknown vulnerabilities. Santamarta (2015) analyzed the firmware and software of an in-market VDR and discovered vulnerabilities that were exploitable. Additionally, VDRs were found to be vulnerable to attacks involving malicious USB drives, leading to breaches, tampering, and deletion of data affecting the Confidentiality-Integrity-Availability (CIA) Triad principles (Vineetha Harish et al., 2022; Hopcraft et al., 2023). Attempts have also been made to secure VDRs to address these security challenges (Seong & Kim, 2019). In Balduzzi and Wilhoit (2014), the authors evaluated the security of AIS by identifying and introducing various software-based and radio-frequency based threats. These types of publications are examples of papers generating new knowledge through experiments.

### 3.2 Scope of assessments

As most of the assessments were technical, that is the focus of this section. However, the scope of the assessment for policy would likely consider organizational, regional, and international scopes. This may also be narrowed to a type of asset or device, and possibly by age as well. The scope of assessment of training would also likely be tied to the participants and types of training; however, this is likely a future piece of work and is, therefore, outside the scope of this literary review on previous studies.

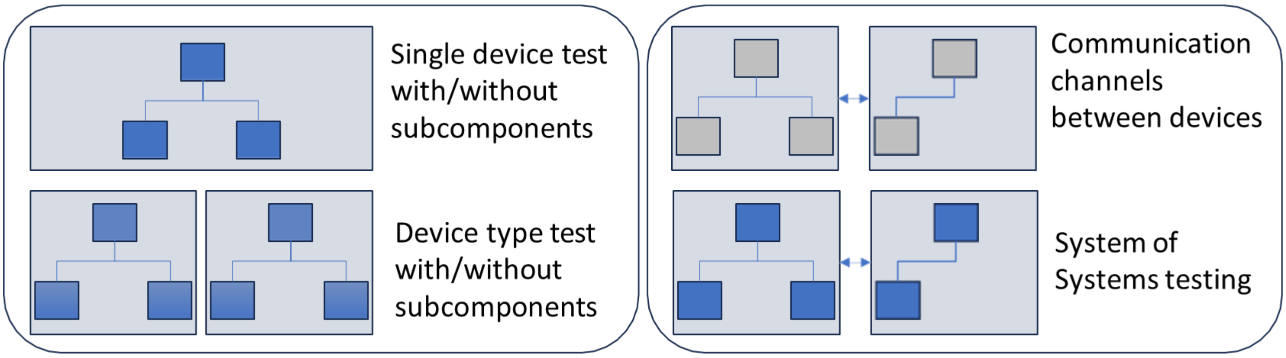



**Figure 4** Scope of assessment for technical assessment. Devices and device sub-components can also be divided into software/hardware components.

### *3.2.1 One device type*

Most of the experiment-based literature revolved around testing a single device (see **Figure 4**). Some examples of VDRs and VSAT, above, took that approach. A few went even further, looking at only the software or firmware of devices, often running in an emulator or virtual machine. For example, a software system used by almost one hundred container terminals worldwide was analyzed in-depth by Eichenhofer et al. (2020) over the course of seven months. A low-level code review was included, which was unusual. However, despite the focus on a single piece of the software, two software modules were isolated for testing: a web application for communicating yard tractor jobs to operators, and a web system with information about ship schedules, container locations, dangerous goods locations, and loading/discharge lists, and used for communicating port status and managing access to external stakeholders.

In a similar way that other studies have examined specific modules within a larger piece of software, tests on maritime system sub-components have been done. There have been on-bridge security tests, in which the sub-components of an ECDIS were tested to find vulnerabilities in third-party components (Svilicic et al., 2019b). Similar tests were performed on other different systems and sub-components like RADAR (Svilicic et al., 2020b; 2019a; 2020a). These experiment papers widen the scope outside one device, and the different vulnerabilities of a system's components.

Botunac and Grzan (2017) analyzed several AIS configurations and introduced a software-based threat. These setups included nineteen combinations of hardware (AIS transponders, receivers), and software were tested in a controlled environment Khandker et al. (2022). This, again, expanded a single-device test, and sought to examine vulnerabilities of a type of system, expanding the scope. A total of eleven types of AIS attacks, including spoofing, jamming, alerts, data encoding, visual disruption, and denial of service, were tested against these setups, and most attacks were successful.

### *3.2.2 Device communication channels*

Outside single devices, or a device and its sub-components, another aspect to consider is communication between devices. For example, the work in Kessler (2021) explained vulnerabilities in the maritime Controller Area Network (CAN) bus communication protocol and NMEA 2000 standards in terms of the CIA triad of information security. In the study, it was mentioned that neither NMEA 2000 nor CAN Bus addresses confidentiality issues. CAN Bus does have bit integrity checks, but neither of them has time stamps; thus, no timing checks. They also do not have any authentication mechanism, and are susceptible to denial of service (DoS) attacks; however, this could be improved by employing cryptographic encryption or network-based intrusion detection systems to filter out malicious messages.

***3.2.3 Systems of systems***

The final and widest scope of assessment is often termed as system-of-systems. This is, essentially, a combination of the previous scopes, including multiple systems, their subcomponents, and multiple connectors and connector types. For example, Tam et al. (2021a) examined an attack chain that reached from the bridge of a ship to the steering mechanisms. While the system-of-systems can be any set of ship or port systems, another well-known term is the Integrated Bridge System (IBS), which is the system of all bridge systems, and is often sold as a single unit to ships by single manufacturers. In an examination of IBS vulnerabilities, including individual components, Awan and Al Ghamdi (2019) found that 43 % of the evidences were related to AIS, GNSS, and sailing directions, out of the 59 evidences collected. Work in Lund et al. (2018a, 2018b) tested the security and integrity of Integrated Navigation Systems (INS), networks of interconnected navigational equipment. In another work around the INS, Svilicic et al. (2019c) tested a vessel's INS using a commonly available vulnerability scanner.

***3.2.4 Time frame***

Another aspect of the scope of an assessment is whether it examines the past, or attempts to examine the future. While most horizon scanning tends to be employed in positional papers, due to the lack of information, these are often near-future assessment for emerging technologies. In the maritime sector, two worthwhile mentions are Maritime Autonomous Surface Ships (MASS) and Artificial Intelligence (AI). Several research studies have been recently conducted on using machine learning and AI in maritime systems, be it for traffic management, collision avoidance, or autonomous ship driving (Kretschmann et al., 2020; Munim et al., 2020). It is important to consider cyber security and testing of MASS and their systems while they are still in the research and development stage (Tabish & Chaur-Luh, 2024; Cho et al., 2022).

In Zagan et al. (2022), it was claimed that Remotely Operated Vessels (ROVs) and MASS could have vulnerabilities in their hardware, software, firmware, and other interconnected components. It explored different types of MASS and their cyber vulnerabilities, and presented a case study of testing BlueROV from Blue Robotics, including mapping its vulnerabilities to CVEs. In contrast, in the article by Walter et al. (2023), the authors experimented with adversarial AI attacks, testing how robust AI object detection can be used against data poisoning, backdoor attacks, patch attacks, and model stealing. This was done both in a lab environment and in situ with real MASS in sheltered waters. Additional tests in Walter et al. (2024) continued to test AI-based computer vision vulnerabilities from the vulnerabilities in the system training AI.

***3.2.5 Human Machine Interaction (HMI)***

Lastly, while machine-to-machine tests have been discussed, the human element is still prominent in the discussions about MASS and ROC. This often uses terms such as Human-in-the-loop (HITL) or Human-Autonomy-Teaming (HAT). For example, Misas et al. (2024) looked at trust in MASS environments from a human perspective, taking into consideration a reduction of Situational Awareness and HAT in remote operations. More generally, an assessment of the risk of MASS operations was conducted by Chang et al. (2021) by conducting reviews of the literature and expert interviews, followed by an analysis and quantification of data using Failure Modes and Effects Analysis (FMEA) combined with Evidential Reasoning (ER) and Rule-based Bayesian Networks (RBNs). A similar study used a novel method of FMECA-ATT&CK-ATLAS (FAA) for the assessing the risks of autonomous cargo vessels. It combined Failure Modes, Effects, and Criticality Analysis (FMECA), MITRE Adversarial Tactics, Techniques, and Common Knowledge framework (MITRE

ATT&CK), and Adversarial Threat Landscape for Artificial Intelligence Systems (ATLAS) (Yousaf et al., 2024).

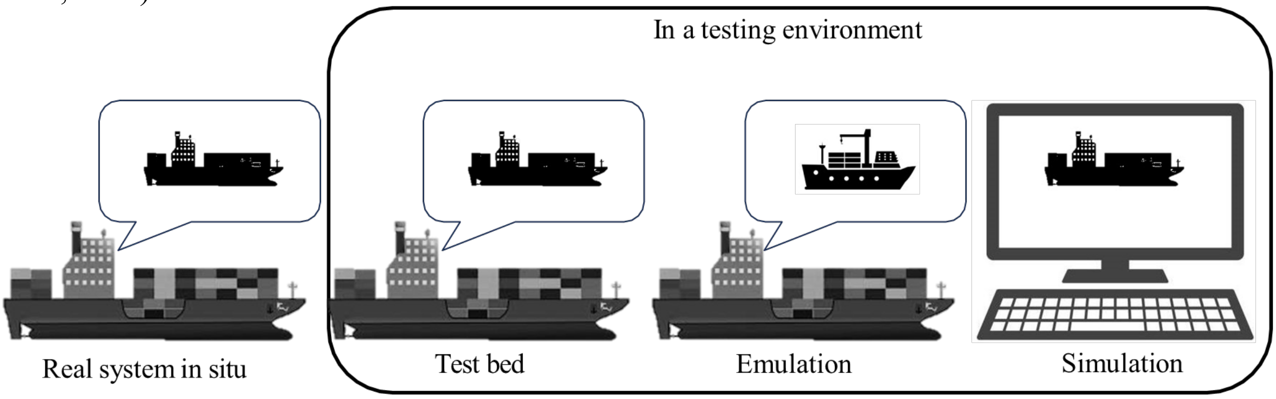



**Figure 5** Basic difference between real systems (software on intended hardware) emulation (hardware/software that enables a system to behave like another) and simulation, which a completely virtual version typically running on generic hardware.

### 3.3 Experimental setups

Once the type (e.g., penetration) and scope (e.g., single device, software only) of the test have been chosen, there are a few more details to choose to determine how a technical test is to be conducted. To better facilitate testing in all scopes, research has been done on creating test beds and environments where penetration tests and vulnerability assessments can be conducted. This has been shown to provide better monitoring, repeatability of experiments, and protection for both the devices in the test environment and outside. There are several companies that offer maritime penetration testing services and consultancy on client ships: Pen Test Partners (2024); Aptive (2024); SHIP IP (2024); Firesand (2024). While this can be useful, the risk to the ship means that a smaller scope of testing is usually executed, yielding realistic results but a subset of the actual vulnerabilities. Tam et al. (2019) discussed this need for a risk-free environment for testing in 2019. Since then, more papers on new experimental environments have been published, discussing simulated, emulated, in situ, and hardware testbed environments. **Figure 5** shows the differences between real systems (test beds included) emulation and simulation in a lab, and real systems in situ, or in their normal operational context.

The work of Longo et al. (2023) presents a virtual environment that can simulate onboard sensors, IBS, and hydraulic systems, and can be connected to external components like ship simulators. Work in Wolsing et al. (2022) modelled a simulated bridge environment using a radar unit, display, and various sensors, and Sicard et al. (2022) developed an ICS physical testbed for French Naval Defense obscurity with a modelled warship with Human Machine Interface (HMI), PLCs for propulsion and artillery units, and other SCADA systems. This setup was useful for testing a French Navy ship; however, its setup and testing are limited to one configuration. A more configurable hardware testbed was proposed in Tam et al. (2019), which allows many ship networks and devices to be connected, the way ships of different types and ages would. A list of software and equipment that could be used in a testbed for autonomous systems was first proposed in Amro and Gkioulos (2021).

In addition to the environment of the experiment, the tests themselves are critical. In other disciplines, like structural and software engineering, there are often a suite of tests that are used to assess aspects of the subject. In a similar way, there have been proposals for cyber security tests for experiments, ranging from generic ones from other industries to sector/device/protocol-specific ones. The authors of Hemminghaus et al. (2021a) developed a tool to implement multiple cyber attacks, such as spoofing, AIS attacks, and Meanie in the Middle (MITM - originally Man in the Middle) attacks against Integrated Bridge Systems. The tool can be used to assess the security of these systems and identify vulnerabilities, but attacks are crafted and offered with the assumption that navigational data will be verified by humans, and that there will be a human in the loop. In spite of the tool itself not being a penetration testing tool, the attacks generated can be used to launch tests through its interactive HMI.

In Vineetha Harish et al. (2024), a sector-specific tool for the maritime bridge environment automatically identified and profiled devices for audits and tests. This brought more functionality to the testbed it was designed to work on, and is an indication of the sub-topic of the field maturing. The authors in Yi and Kim (2021) proposed a security testing approach for naval combat system, a complex software-based system, that connects various heterogeneous systems, including sensors, weapons, networks and navigation systems. The authors chose to develop a software-specific security testing framework as these systems were increasingly being used commercially. Studies researching training would need to be clear in their training environment (e.g., online, real time, real ship, simulation); however, previous studies have chosen these for experiments, not necessarily assessments of students or the training itself.

## 4. New knowledge papers: Solutions

As defined earlier, when a paper does more than provide a proposal within a positional paper, this paper considered it a new knowledge paper that provides a solution. This can be at several levels, and at a minimum a solution is a more detailed proposal, but ideally these papers will have trailed a test case, or undergone more vigorous verification. In addition to the level of readiness, the type of solutions is critical. In our review of the existing literature, these tend to be frameworks (e.g., training, risk assessment) or research enablers (e.g., cyber ranges, test beds).

### 4.1 Existing security testing frameworks

From 2013 - June 2024, a small percentage of the existing literature focused on security testing and assessment frameworks for the maritime industry. Most of what is available relate to threat assessment in the maritime sector, rather than actual security testing methods like pentesting or vulnerability assessments. The authors in Enoch et al. (2021) acknowledged that automated security modelling and vulnerability assessments can help improve cyber resilience in the sector and, given the differences in the environment and type of systems, current IT and Internet of Things (IoT) network assessments may not be able to be seamlessly integrated into the maritime sector. To address this issue, the authors presented the Maritime Vessel-Hierarchical Attack Representation Model (MV-HARM), a graphical security model of ships. The model can be used to assess the effects of an attacker, both on single and multiple targets, identify potential attack paths with attributes such as network configurations, vulnerabilities, systems, and connectivity, and assess the effectiveness of defense strategies on the networks.

Similarly, Pitropakis et al. (2020) proposed a framework to collect and analyze maritime cyber threat intelligence as a solution to the lack of threat awareness in the sector. The MAritime Threat INtelligence FRAMEwork, also known as MAINFRAME, collects and correlates data, audits data integrity using Hyperledger blockchain and honeypots, performs threat intelligence using a Security Information and Event Management (SIEM) system, and machine learning models, and is integrated into VERACITY, a commercial product from DNV GL. The authors Melnik et al. (2023) discussed the importance of vulnerability and security assessments for the maritime sector and propose a probabilistic assessment of a vessel's cyber security considering targeted and non-targeted cyber threats. Yoo and Park (2021) proposed a qualitative solution to determine item-specific vulnerabilities to identify cyber risks in the sector. They conducted a qualitative risk assessment with a group of six experts, who reviewed twenty-seven risk factors divided into three groups of administrative risks, technical risks, and physical security risks, to derive cyber security improvement plan priorities. The study also emphasized the need to include quantitative vulnerability assessment of the elements to calculate quantitative risks.

While previous frameworks have provided solutions, many were manual paper-based exercises, not verified, or both. An example of a simulation-based security tool is the Bridge Attack Tool (BRAT), which implements several attacks against IBS to help in security assessments (Hemminghaus et al., 2021a). The authors pointed out that, in the maritime sector, there is not a sector-specific tool, that testers often use generic tools to carry out assessments, and that there is a need for maritime-specific testing frameworks. BRAT uses preconfigured attacks like AIS attacks against IBS and uses an interactive Human Machine Interface. Its results are not verified such as, for example, it was not verified with real data or on real hardware.

The types of papers above were popular in the early 2000s; however, as the state of the art grew, the novelty of these papers decreased. Due to this, as of 2023, more papers are now needed to expand the state-of-the-art by automating tools and/or verifying the results of the testing framework. A prime example of this is BridgeInsight, mentioned previously (Vineetha Harish et al., 2024), which pushes the boundaries of testing frameworks by both automating tests, moving away from manual inputs, and also verifying its results by testing the security vulnerabilities on real hardware.

### 4.2 Risk assessment/Management

Within the last decade of maritime cyber research, risk assessment methods and crew awareness make up a significant section of frameworks proposed in the literature. There is, therefore, a need to research and develop new and better tools and frameworks to test the systems and standardize and regulate the frameworks across the sector.

One of the earlier maritime cyber-risk papers was concerned about maritime supply chains and critical infrastructures (Polemi & Papastergiou, 2015). The document itself was a review paper, but the projects it summarized were new solutions in the field, namely CYSM, Medusa, and Mitigate. These solutions examined a port's cyber-physical elements and supply chain risks (Polemi & Papastergiou, 2015). Between 2018 - 2022, a considerable number of studies like this were conducted.

In Polatidis et al. (2018), its authors conducted discussions about MITIGATE, the risk management system mentioned above, which is used to discover cyber attack paths and detect and address risks based on parameters such as entry points, target points, attacker capability, and propagation length. In dynamic supply chain environments, attack path discovery helps identify flaws and can be fed into the wider risk management system. The authors also claimed this approach can be used to assess risks in SCADA systems as well Kalogeraki et al. (2018).

Tam and Jones (2019) introduced dynamic risk analysis through MaCRA (Model-Based Framework for Maritime Cyber-Risk Assessment) to quantify and assesses risks. Through MaCRA, maritime cyber risks can be quantified by modelling attributes such as attacker abilities, ease of exploit, attacker rewards, and target vulnerabilities. Results are projected on a simple risk quadrant. This framework has also been applied to profile and quantify risks in autonomous ships and maritime ports infrastructure. The authors provided fine-grained but theoretical assessments of the risks and also of the potential econometric and cascading cyber-physical impacts (Tam et al., 2021b).

While several of the academic literature discussed in this section either modified or created new solutions and knowledge due to limitations in adapting other methods to maritime, many other studies have used existing frameworks, and then fed expert data into those frameworks, for results. However, from this paper's comprehensive review, many of these studies relied on a very small set of experts (see **Figure 6**) and/or did not disclose their metrics for "expertise" in sufficient detail. Therefore, while useful contributions, the authors of this paper considered papers of this nature to be a type of systematic review of expert opinions, rather than adding new knowledge.

### 4.3 Technical solutions

Previously, most solutions proposed were self-labelled as frameworks and models. These were not technical in nature, but did address technical topics. In Jacq et al. (2018), the authors discussed the possible solutions to cyber security challenges by investigating the People, Process, Technologies (PPT) triad.

Considering the last decade of research, the maritime sector is still in the early stages of testing for cyber security, which means that there are limited technological solutions to the cyber security challenges it faces. Many papers are still positional papers, or early proposals for non-technical solutions. More technically, some research has been conducted to secure widely used protocols in the sector, such as the Automatic Identification System (AIS), and most of the solutions have been based on cryptographic techniques and digital certificates (Goudossis and Katsikas, 2019). That research proposed a secure AIS model that uses techniques like Identity-Based Public key cryptography and symmetric cryptography to encrypt AIS messages and anonymize data.

In a related study, SecureAIS, proposed by Aziz et al. (2020), is a software-based key establishment protocol designed to encrypt and authenticate messages between AIS transceivers using cryptography techniques such as the Elliptic Curve Qu-Vanstone (ECQV) implicit certification scheme and the Elliptic Curve Diffie-Hellman (ECDH) key agreement algorithm. The authors also demonstrated a proof-of-concept using SDRs and GNURadio. In their experiments, they observed that the solution reduced the time overhead by 20 % using only twenty AIS time slots, compared to traditional X.509 certificates. SIGMAR is a framework designed to add authentication to nautical datagrams using digital signatures based on asymmetric cryptography (Hemminghaus et al., 2021b). The authors of the framework have identified the issue that changing or replacing maritime systems can be expensive and difficult and, thus, retrofitting features is the best way, especially when the systems have too low computational power to perform intensive operations like encryption.

Solutions discussing attack detection and Intrusion Detection/Prevention systems are also becoming prevalent. Studies have been conducted to deploy such attack/threat detection solutions in IoT-based Maritime Transportation Systems (MTS), and these solutions are modelled using different learning algorithms (Liu et al., 2023; Gyamfi et al., 2023). Merino Laso et al. (2022) presented the idea and results from the European project ISOLA (Innovative and Integrated Security Systems on Board Covering the Life Cycle of a Passenger Ships Voyage), developed within the scope of the Horizon2020 program, with the aim of identifying threats and risks and assessing them, as well as incorporating incident detection and reporting, focusing on cruise ships. There are several modules in the ISOLA platform, such as sensor data processors, artificial intelligence algorithms for dynamic vulnerability detection, intrusion detection systems, warning systems, and integration of open-source tools for finding flaws. The authors mentioned that the platform will provide insights to users during incidents and crises to help improve the response, and mentioned the need for a dynamic cyber security vulnerability assessment tool to be developed in the future.

### 4.4 Crew awareness training/ frameworks

A critical part of ensuring resilience in the maritime sector is training crew members and operators in cyber awareness. With the increasing digitization in the field, and the integration of new systems into navigation and communication networks, it is crucial to educate people on how to better identify, respond to, and protect against cyber threats and attacks. Ship Bridge Simulator-based training is the most common method for cyber awareness training in the maritime sector, and there have been several examples of research that have supported this. As part of a maritime ship simulator-based exercise, students encountered cyber threats related to OSINT and digital footprint at sea, which helped them gain a better understanding of cyber hygiene and the use of technology at sea (Yousaf et al., 2024). Erstad et al. (2023) demonstrated the benefits of a Human-Centred Design approach when developing a simulator-based incident scenario for maritime cyber resilience training, and stressed the effectiveness of simulators as a learning environment. These were also tested in a real mariner training environment with a focus on Norwegian cadets.

Another popular method for maritime cyber awareness training is through cyber ranges. Tam et al. (2021c) discussed the use of cyber ranges, physical test beds, simulations, and emulations in training contexts and how they may have different pros and cons. This was written out of the Cyber-MAR EU project (CyberMAR, 2024). The same project was also published in Pyykko et al. (2020), which argued that a holistic model using cyber ranges with realistic scenarios can improve the efficiency of the maritime cyber operations. Cyber range-based training can be effectively executed by developing an architecture or model designed to consider levels of simulation and realism according to the audience and scenario. A maritime cyber range was proposed by Potamos et al. (2021), comprising simulated and emulated communication networks, administration tools, navigational equipment, and machinery, to assist in cyber awareness training by means of attack simulations. Additionally, it can be integrated into a larger Multi Domain Cyber Range Federation to share resources between geographically distributed cyber ranges and develop multi-domain cyber training scenarios. As explored more in a later section, this is a relatively new subject within maritime cyber security, but one that has seen significant growth in just a few years.

## 5. Review papers

Within the set of review papers published in the last decade, there were three distinct types identified. First were general review papers, where the authors selected papers by region, subject, or out of interest. These were often self-labelled as reviews, surveys, and overviews. Other papers claimed themselves to be systematic reviews, which were reviews that adhered to more strict rules and systematic procedures. However, while many claimed to be systematic, in actuality, many were more accurately general review papers, as discussed below. Lastly, the authors had previously defined papers that used existing frameworks and used them to process/review expert opinions that were limited (small) and/or without robust discussion on what they considered "an expert" and if the range of necessary expertise was involved. Instead of considering these as new contributions to knowledge, these were classified as reviews of opinions instead of reviews of papers.

### 5.1 Limitations of literature reviews

While literature reviews of all kinds can add to the overall knowledge, there are several limitations to survey papers in maritime cyber security that should be considered. The first limitation, which is illustrated in the discussion, is that the majority of the papers in maritime cyber security in the last five years have been overwhelmingly survey papers, reducing the novelty of each publication. In addition, due to how few papers have been produced, especially new knowledge papers, most, if not all, reviews published before 2024 were limited and biased due to the small set of available concrete research since 2013; however, the papers did not fully disclose this limitation, leading readers to potentially wrong assumptions. Many also restricted their set further by excluding articles in certain languages or from certain publication venues, despite their impact or high citations.

Another significant limitation to many previous reviews, especially the systematic ones, is that frameworks tend to work best on distilling an extensive body of work that has established journals and common terminology. These assumptions do not hold as well in a new body of research. Firstly, as seen in this paper's analysis of the literature, most early positional papers before 2017 - 2018 were published in a wide range of conferences, journals, and venues. Therefore, excluding papers outside of high impact journals, while reasonable for an established field, limits the understanding of a new growing research topic that has not been widely published. On the second point, as seen with Google trends, doing a systematic review based on terms at this point is also difficult, as many publications are early positional papers from different countries and subjects and across academia, industry, and government. Common terms and phrases have not yet been well established. In this comprehensive review, all papers related to maritime cyber security, even if they use different terms (e.g., ship vs vessel, cybersecurity vs cyber security) have been considered.

Another important note when considering review papers listing previous, publicly known, attacks is that currently the majority of them are only focused on publicly released information and those released in a single language such as English. This is a concern, as Lund et al. (2018a);

Mrakovic and Vojinovic (2019) pointed out how under-reporting is a significant issue. This research also discusses the low awareness of what different types of cyber attacks look like, indicating that the reports that are known are limited and often biased towards very easily recognized attacks like DoS and ransomware. This is one of the critical limitations of review studies based solely on public incidences for information. Therefore, while useful indicators that cyber attacks are happening in the sector, they may not be fully representative of all the attacks happening.

While there are limitations applying systematic reviews to a new area of research, it is important to highlight limitations of comprehensive reviews as well. A comprehensive literature review summarizes a body of work, and while the freedom to choose key works is essential, there is a possibility of author bias. In this review, the authors attempted to mitigate this by using publication dates to highlight new, field-defining areas of research as they were developed and explored. However, there is possible bias towards research the authors are familiar with, and this should be considered by the reader. It should also be noted that the database used for the literature search is Google Scholar, which pulls articles from most of the academic databases like Semantic Scholar, Scopus, and Web of Science. Google Scholar helped the authors to understand the field by gaining a broader understanding, as the review included not just academic articles, but also technical reports, theses, and books.

### 5.2 Limitations of expert reviews

This review also includes the use of existing frameworks to rephrase information as a type of review, just a more formalized or systematic one. For example, the MITRE ATT&CK framework was used by Jo et al. (2022) to analyze and model cyber threats on ships, where the authors analyzed four known cases from other literature. The cases were then analyzed with the existing MITRE ATT&K model and were mapped to phases like initial access, execution, and command and control. In another example, Kayisoglu et al. (2022) performed risk assessments of navigation systems using widely accepted frameworks that are also popularly used to uncover vulnerabilities and threats. The same core authors that used Failure Modes and Effects Analysis (FMEA) to assess the risks on Voyage Data Recorders Soner et al. (2023), also conducted a quantitative human risk assessment on AIS data and systems using the Shipboard Operation Human Reliability Analysis (SOHRA) method (Soner et al., 2024). The same core authors again, in Kayisoglu et al. (2024) developed treatment and mitigation strategies for onboard RADAR systems using the CORAS framework to perform the risk assessment.

The limitation of many existing reviews is that they often have very small groups of people, the groups are biased, or there are no essential details about the experts provided. In the author's survey of 319 papers, the smallest group of experts was four. The largest was 239; however, that was an anonymous online survey, with no verification or assessment of the participants' expertise. Moreover, in the author's analysis, all papers with more than seventy responses reported collecting anonymous options and/or not verifying any responded details. Many others with below seventy participants were also unclear or reported no verification or of not assessing experts. As seen in **Figure 6**, while the average of participants in all papers interviewing or surveying people was roughly seventy, about a third of all such papers had less than ten participants and, if only looking at studies that claimed (not necessarily verified) that participants were "experts", that average falls closer to twenty participants per study.

Another point of consideration is that several of these types of papers were published by the same core authors, which makes it possible that the same group of experts might have been used for multiple studies. This is not made clear in the studies, and can unintentionally create bias in a body of work, especially when review articles make assumptions and overstate certain findings in their summaries and discussions.

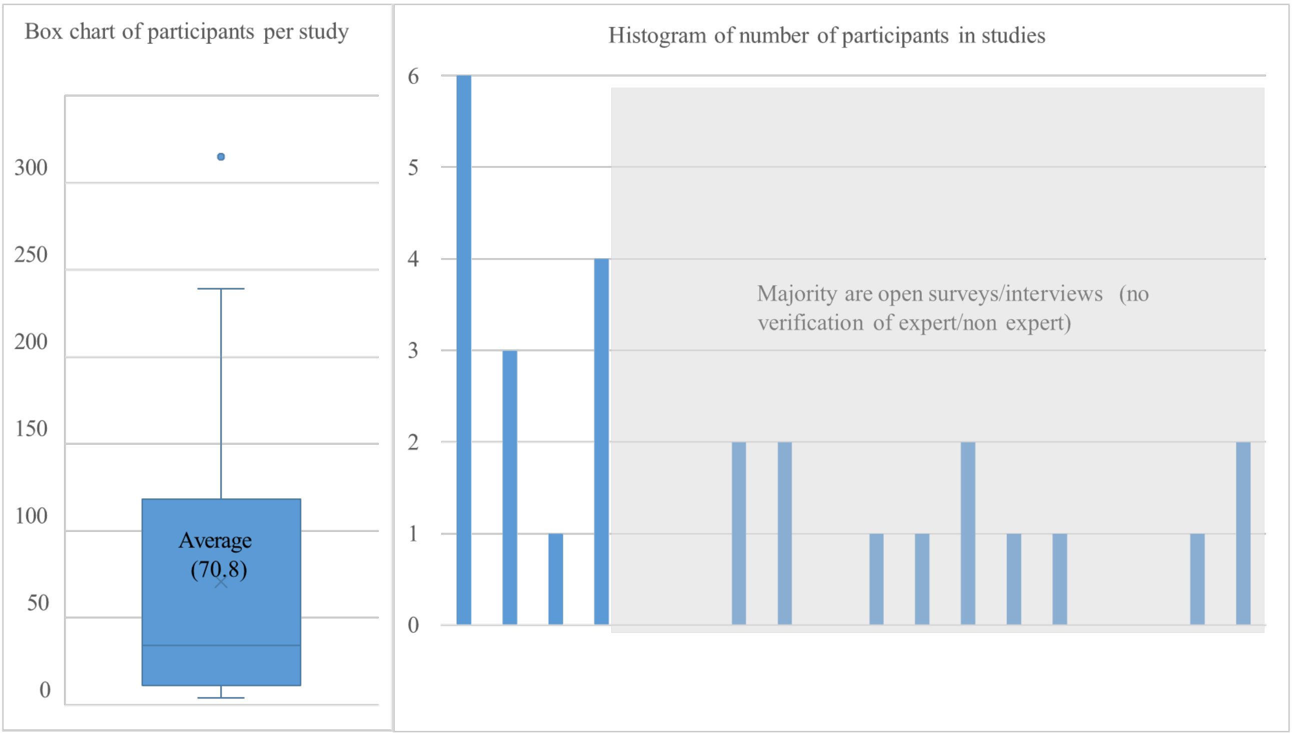



**Figure 6** Participants in past maritime cyber security surveys/interview studies.

## 6. Discussion

This review aims to examine how maritime cyber security research has matured in its "first" decade of existence. This time frame was determined by looking for the first piece of literature that was dedicated to the concept of maritime cyber security, and was not just a side note in another topic. It did not exclude papers based on the venue of publication or language, unlike similar works. As a result, this review considered 319 papers. While this did cover a wider range of papers from previous reviews, there were potential biases which the authors explained and tried to mitigate, as per in Section 5.1. This review also had a clear cut-off for the end for 2023; future work would need to include publications in 2024, once that year has been completed. As the majority of these were positional and survey papers, it was not felt there were enough foundational articles to conclude anything about how secure the sector is, etc. However, this discussion can highlight some aspects of the maturity of this research area in a way that can help guide those just entering the field, those already working in it, and those looking for ways to progress the state of the art. These are summarized in the discussion points below:

1) Global interest in maritime cyber security continues to grow, both in academic research and in the public eye. A steady number of major public reports of attacks on maritime assets, globally and annually, is likely a factor in this visibility and interest, as discussed in the Introduction. Interestingly, many internal reports of cyber attacks not publicly disclosed show a much more dramatic increase of incidences, up to 86 % in some years and in some locations (US Coast Guard (2022)). This indicates that the sector still does not have a full grasp on how extensively cyber attacks are happening in the maritime sector, which also links back to both people's awareness and digital forensics.

2) One concern is the ratio of review papers to other types of papers, as seen in **Figure 2**. From 2013 - 2016, in the comprehensive assessment, there were only positional papers and review papers. Many review papers then were reviews of a few ideas, not facts or experimental results, and content from other sectors. Because of the ambiguity of the input, the results of many of these reviews were, therefore, unclear. There was a significant spike in review papers from 2017, with many of the

earlier ones again more summary than review because there were very few pieces of concrete study to review as a body of work. From 2019 to the end of 2023, review papers were the number one type of publication. As discussed before, this causes some concern, as it seems most papers in the field seemed to review a very small number of foundational articles, reviewed other reviews, or included studies outside the field. Many of the reviews reduced the available number of papers in the review further with metrics that created bias (e.g., language). This situation is dangerous, as it can create echo chambers, bias, and ideas that may eventually be reported as undisputed fact, when they have not been fully researched yet. The authors would urge researchers to focus more on generating new knowledge articles in order to grow a more scientific body of work.

3) The breakdown of the umbrella topic of maritime cyber security into specialist areas (see **Figure 3**) has shown the research growing in terms of breadth and depth. Although not shown in the figure itself, many of the positional papers that helped broaden the scope and define sub-topics more clearly are from a wide range of researchers globally. Initially, from 2013 – 2016, there were very few branches of maritime cyber security besides ports, or the research took a very high-level and generic view. In 2016, the discussion of ships was brought up separately from port security and, from 2017 to 2024, there have been multiple new areas proposed for research. Generally speaking, most of these positional papers have also been followed by new knowledge papers, indicating growth. It is the authors' opinion that the breadth and depth of new knowledge papers is progressing well as a result of a comprehensive review of key papers that actively push the state of the art.

4) In addition to proposing more new knowledge papers, it is also worth discussing how to increase the breadth of knowledge. The majority of experiments to test the cyber security of devices, for example, have focused on AIS, ECDIS, and VDR, with a few on RADAR or a PLC. Each of these papers have mentioned that the device focused on is one device in a rich ecosystem of other devices, but the focus has continued to stay very narrow. There is also scope for more verification and assessment of the tools and frameworks being proposed. At the moment, most of the frameworks are manual, but ways to verify the frameworks' work, verification for automated tools made, and verification for successful training would seem beneficial ways to grow the body of research further. It would also be beneficial to broaden research into other maritime infrastructure, such as underwater sea cables and offshore structures (e.g., oil rigs, wind turbines).

## 7. Conclusions

Compared to other fields of research, maritime cyber security is still a new area of research. In its "first decade" of existence, it has seen global interest, and that interest has defined and shaped it and its subtopics through positional papers, and then explored those topics with experiments, frameworks, and solutions in more depth and with scientific rigor. Literature reviews have also been published, attempting to phrase the challenges and solutions to various audiences. This article provides a comprehensive review, as opposed to a general or systematic review, at an appropriate time when the body of work is sufficiently mature enough. While overall the maturity of the field has clearly progressed from its early stages, there are areas of development and concern, which are likely normal in a new area. These may resolve naturally; the findings of this review on gaps in the research, and concern on research efforts globally, are meant to help guide the next decade of maritime cyber security research productively.

## Acknowledgement

This research was part of the Cyber SHIP lab project at the University of Plymouth. The authors are grateful to the project funder- Research England- and our industry partners, who supported our research by providing valuable insights. The authors would like to thank the colleagues from the Cyber SHIP lab, for their invaluable support and comments on the earlier drafts.

## References

Al Ali, N. A. R., Chebotareva, A. A., & Chebotarev, V. E. (2021). Cyber security in marine transport: Opportunities and legal challenges. *Scientific Journal of Maritime Research, 35*(2), 248-255. https://doi.org/10.31217/p.35.2.7

Amor, A., & Gkioulos, V. 2021. *Communication and cybersecurity testbed for autonomous passenger ship* (pp. 5-22). European Symposium on Research in Computer Security. Springer. https://doi.org/10.1007/978-3-030-95484-0_1.

AP Moller - Maersk. (2017). *The Annual Report for 2017 of A.P. Moller - Maesk A/S*. Retrieved from https://investor.maersk.com/system/files-encrypted/nasdaq_kms/assets/2018/04/25/13-00-21/A.P._Moller_-_Maersk_Annual_Report_2017.pdf

Aptive. (2024). *Maritime penetration testing services*. Retrieved from https://www.aptive.co.uk/penetration-testing/maritime

Arghire, I. (2023). *Ransomware gang publishes data allegedly stolen from maritime firm Royal Dirkzwager – Security Week*. Security Week. Retrieved from https://www.securityweek.com/ransomware-gang-publishes-data-allegedly-stolen-from-maritime-firm-royal-dirkzwager

Awan, M. S. K., & Al Ghamdi, M. A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *Journal of Marine Science and Engineering, 7*(10), 350. https://doi.org/10.3390/jmse7100350

Aziz, A., Tedeschi, P., Sciancalepore, S., & Pietro, R. D. (2020). *SecureAIS - Securing Pairwise Vessels Communications* (pp. 1-9). In Proceedings of the 2020 IEEE Conference on Communications and Network Security. Avignon, France. https://doi.org/10.1109/CNS48642.2020.9162320

Balduzzi, M., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system (pp. 436-445). In Proceedings of the 30$^{th}$ Annual Computer Security Applications Conference. New York, USA. http://dx.doi.org/10.1145/2664243.2664257

BIMCO. (2021). The guidelines on cyber security onboard ships. *International Chamber of Shipping, 4*, 1-53. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection. 39*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Botunac, I., & Grzan, M. (2017). Analysis of software threats to the automatic identification system. *Shipbuilding: Theory and Practice of Naval Architecture, Marine Engineering and Ocean Engineering, 68*, 97-105. https://doi.org/ 10.21278/brod68106

Chambers, S. (2022). *Voyager worldwide hit by cyber attack*. Splash. Retrieved from https://splash247.com/voyager-worldwide-hit-by-cyber-attack

Chang, C. H., Kontovas, C., Yu, Q., & Yang, Z. (2021). Risk assessment of the operations of maritime autonomous surface ships. *Reliability Engineering & System Safety, 207*, 107324. https://doi.org/10.1016/j.ress.2020.107324

Chia, R. Y. (2019). *The need for ethical hacking in the maritime industry* (pp. 108-121). Time for a New Maritime Era - Society of Naval Architects and Marine Engineers Singapore.

Cho, S., Orye, E., Visky, G., & Prates, V. (2022). Cybersecurity considerations in autonomous ships. Retrieved from https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf

CyberMAR. (2024). *About - Cybermar*. Retrieved from https://www.cyber-mar.eu/about

Eichenhofer, J. O., Heymann, E., Miller, B. P., & Kang, A. (2020). An in-depth security assessment of maritime container terminal software systems. *IEEE Access, 8*, 128050-128067.

https://doi.org/10.1109/ACCESS.2020.3008395
Enoch, S. Y., Lee, J. S., & Kim, D. S. (2021). Novel security models, metrics and security assessment for maritime vessel networks. *Computer Networks, 189*, 107934. https://doi.org/10.1016/j.comnet.2021.107934
Erstad, E., Hopcraft, R., Harish, A. V., & Tam, K. (2023). A human-centred design approach for the development and conducting of maritime cyber resilience training. *WMU Journal of Maritime Affairs, 22*, 241-266. https://doi.org/10.1007/s13437-023-00304-7
ESC Global Security. (2015). *Maritime cyber security white paper: Safeguarding data through increased awareness*. Retrieved from https://allaboutshipping.co.uk/wp-content/uploads/2015/11/ESCGS-Cyber-Security-WP-2015.pdf
Fenton, A. J. (2024). Preventing catastrophic cyber-physical attacks on the global maritime transportation system: A case study of hybrid maritime security in the straits of Malacca and Singapore. *Journal of Marine Science and Engineering, 12*(3), 510. https://doi.org/10.3390/jmse12030510
Firesand. (2024). *Maritime cyber security services: Penetration testing*. Retrieved from https://www.firesand.co.uk/sectors/maritime-cyber-security-services
Glover, C. (2022). *Port of London authority cyberattack 'politically motivated'.* Tech Monitor. Retrieved from https://techmonitor.ai/technology/cybersecurity/port-of-london-authority-cyberattack.
Goudossis, A., & Katsikas, S. K. (2019). Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology, 24*, 410-423. https://doi.org/10.1007/s00773-018-0561-3
Greig, J. (2022). *Shell forced to reroute supplies after cyberattack on two German oil companies-ZDNet*. Retrieved from https://www.zdnet.com/article/shell-forced-re-route-oil-supplies-after-cyberattack-on-german-companies
Gurren, J., Harish, A. V., Tam, K., & Jones, K. (2023). *Security implications of a satellite communication device on wireless networks using pentesting* (pp. 292-298). In Proceedings of the International Conference on Wireless and Mobile Computing, Networking and Communications. Montreal, Canada. https://doi.org/10.1109/WIMOB58348.2023.10187791
Gyamfi, E., Ansere, J. A., Kamal, M., Tariq, M., & Jurcut, A. (2023). An adaptive network security system for iot-enabled maritime transportation. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2538-2547. https://doi.org/10.1109/TITS.2022.3159450
Harreveld, M. V. (2023). *Russians may hack Zeeland ports*. Retrieved from https://www.bnr.nl/nieuws/binnenland/10516325/russische-hackers-vallen-zeeuwse-havens-aan
Hemminghaus, C., Bauer, J., & Padilla, E. (2021a). Brat: A bridge attack tool for cyber security assessments of maritime systems. *International Journal on Marine Navigation and Safety of Sea Transportation, 15*, 35-44. https://doi.org/10.12716/1001.15.01.02.
Hemminghaus, C., Bauer, J., & Wolsing, K. (2021b). *Sigmar: Ensuring integrity and authenticity of maritime systems using digital signatures* (pp. 1-6). In Proceedings of the 2021 International Symposium on Networks, Computers and Communications. Dubai, United Arab Emirates. https://doi.org/10.1109/ISNCC52172.2021.9615738
Hopcraft, R., & Martin, K. (2018). Effective maritime cybersecurity regulation: The case for a cyber code. *Journal of the Indian Ocean Region, 14*, 1-13. https://doi.org/10.1080/19480881.2018.1519056
Hopcraft, R., Harish, A. V., Tam, K., & Jones, K. (2023). Raising the standard of maritime voyage data recorder security. *Journal of Marine Science and Engineering, 11*, 267. https://doi.org/10.3390/jmse11020267
International Maritime Organization. (2017). *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems*. Retrieved from

https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ResolutionMSC.428(98).pdf

International Maritime Organization. (2022). *Msc-fal.1/circ.3/rev.2 - guidelines on maritime cyber risk management*. International Maritime Organization. Retrieved from https://www.liscr.com/sites/default/files/liscr_imo_resolutions/MSC-FAL.1-Circ.3-Rev.2.pdf

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018). *Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre* (pp. 1-8). In Proceedings of the 2nd Cyber Security in Networking Conference. Paris, France. https://doi.org/10.1109/CSNET.2018.8602669

Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022). Cyberattack models for ship equipment based on the MITRE ATT&CK framework. *Sensors, 22*(5), 1860. https://doi.org/10.3390/s22051860

Jones, K. D., Tam, K., & Papadaki, M. (2015). Threats and impacts in maritime cyber security. *Engineering & Technology Reference, 2016*, 123. https://doi.org/10.1049/ETR.2015.0123

Kalogeraki, E. M., Papastergiou, S., Mouratidis, H., & Polemi, N. (2018). A novel risk assessment methodology for scada maritime logistics environments. *Applied Sciences, 8*(9), 1477. https://doi.org/10.3390/app8091477

Karim, M. S. (2022). Maritime cybersecurity and the imo legal instruments: Sluggish response to an escalating threat? *Marine Policy, 143*, 105138. https://doi.org/10.1016/j.marpol.2022.105138

Kayisoglu, G., Bolat, P., & Tam, K. (2022). *Determining maritime cyber security dynamics and development of maritime cyber risk check list for ships* (pp. 22-27). In Proceedings of the 22nd Annual General Assembly International Association of Maritime Universities. Batumi, Geogia.

Kayisoglu, G., Bolat, P., & Tam, K. (2024). A novel application of the coras framework for ensuring cyber hygiene on shipboard radar. *Journal of Marine Engineering & Technology, 23*(2), 67-81. https://doi.org/10.1080/20464177.2023.2292782

Kessler, G. C. (2021). The can bus in the maritime environment: Technical overview and cybersecurity vulnerabilities. *International Journal on Marine Navigation and Safety of Sea Transportation, 15*(3), 531-540. https://doi.org/10.12716/1001.15.03.05

Khandker, S., Turtiainen, H., Costin, A., & Hamalainen, T. (2022). Cybersecurity attacks on software logic and error handling within ais implementations: A systematic testing of resilience. *IEEE Access, 10*, 29493-29505. https://doi.org/10.1109/ACCESS.2022.3158943

Kretschmann, L., Zacharias, M., Klover, S., & Hensel, T. (2020). *Machine learning in maritime logistics*. Retrieved from https://shipzero.com/wp-content/uploads/2022/12/10015_compressed.pdf

Liu, W., Xu, X., Wu, L., Qi, L., Jolfaei, A., Ding, W., & Khosravi, M. R. (2023). Intrusion detection for maritime transportation systems with batch federated aggregation. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2503-2514. https://doi.org/10.1109/TITS.2022.3181436

Longo, G., Orlich, A., Musante, S., Merlo, A., & Russo, E. (2023). MaCySTe: A virtual testbed for maritime cybersecurity. *SoftwareX, 23*, 101426. https://doi.org/10.1016/j.softx.2023.101426

Lund, M. S., Gulland, J., Hareide, O. S., Jøsok, Ø., & Weum, K. (2018a). *Integrity of integrated navigation systems* (pp. 1-5). In Proceedings of the Conference on Communications and Network Security. Beijing, China. https://doi.org/10.1109/CNS.2018.8433151

Lund, M. S., Hareide, O. S., & Jøsok, Ø. (2018b). An attack on an integrated navigation system. *Necesse, 3*(2), 149-163. https://doi.org/10.21339/2464-353x.3.2.149

Maritime Executive. (2023). *Tokyo mou reports previously-undisclosed cyberattack in 2022*. Retrieved from https://maritime-executive.com/article/tokyo-mou-reports-previously-undisclosed-cyberattack-in-2022

Melnik, O., Onyshchenko, S., Onishchenko, O., Lohinov, O., & Ocheretna, V. (2023). Integral approach to vulnerability assessment of ship's critical equipment and systems. *Transactions on Maritime Science, 12*(1), 002. https://doi.org/10.7225/toms.v12.n01.002

Merino, L. P., Salmon, L., Bozhilova, M., Ivanov, I., Stoianov, N., Velev, G., Claramunt, C., & Yanakiev, Y. (2022). *Isola: An innovative approach to cyber threat detection in cruise shipping* (pp. 71-81). Springer. https://doi.org/10.1007/ 978-981-16-4884-7_7

Misas, J. D. P., Hopcraft, R., Tam, K., & Jones, K. (2024). Future of maritime autonomy: Cybersecurity, trust and mariner's situational awareness. *Journal of Marine Engineering & Technology, 23*(3), 224-235. https://doi.org/10.1080/20464177.2024.2330176

Morrissette-Beaulieu, F. (2023). *Canadian ports victims of cyberattacks by a pro-Russian group*. Radio-Canada. Retrieved from https://ici.radio-canada.ca/nouvelle/1971087/noname057-site-web-ports-canadiennes-pirates-informatiques-prorusses

Mrakovic, I., & Vojinovic, R. (2019). Maritime cyber security análisis: How to reduce threats? *Transactions on Maritime Science, 8*, 132-139. https://doi.org/10.7225/toms.v08.n01.013

Munim, Z. H., Dushenko, M., Jimenez, V. J., Shakil, M. H., & Imset, M. (2020). Big data and artificial intelligence in the maritime industry: A bibliometric review and future research directions. *Maritime Policy & Management, 47*(5), 577-597. https://doi.org/10.1080/03088839.2020.1788731

NCSC. (2022). *Penetration testing*. Retrieved from https://www.ncsc.gov.uk/guidance/penetration-testing

NL Times. (2023). *Dutch ports' websites offline for hours, days due to pro-Russian cyber attacks: NL times.* Retrieved from https://nltimes.nl/2023/06/14/ dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks

Page, C. (2023). *Maritime giant DNV says 1,000 ships affected by ransomware attack*. TechCrunch. Retrieved from https://techcrunch.com/2023/01/18/dnv-norway-shipping-ransomware

Pavur, J., Moser, D., Strohmeier, M., Lenders, V., & Martinovic, I. (2020). A tale of sea and sky on the security of maritime vsat communications (pp. 1384-1400). In Proceedings of the 2020 IEEE Symposium on Security and Privacy. San Francisco, USA. https://doi.org/10.1109/SP40000.2020.00056

Pen Test Partners. (2024). *Maritime cyber security testing*. Retrieved from https://www.pentestpartners.com/penetration-testing-services/maritime-cyber-security-testing

Pitropakis, N., Logothetis, M., Andrienko, G., Stefanatos, J., Karapistoli, E., & Lambrinoudakis, C. (2020). Towards the creation of a threat intelligence framework for maritime infrastructures. *Lecture Notes in Computer Science, 11980*, 53-68. https://doi.org/10.1007/978-3-030-42048-2_4.

Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces, 56*, 74-82. https://doi.org/10.1016/j.csi.2017.09.006

Polemi, N., & Papastergiou, S. (2015). *Current efforts in ports and supply chains risk assessment* (pp. 349-354). In Proceedings of the 10th International Conference for Internet Technology and Secured Transactions. London, UK. https://doi.org/10.1109/ICITST.2015.7412119

Potamos, G., Peratikou, A., & Stavrou, S. (2021). *Towards a maritime cyber range training environment* (pp. 180-185). In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR). https://doi.org/10.1109/CSR51186.2021.9527904

Pyykko, H., Kuusijarvi, J., Noponen, S., Toivonen, S., & Hinkka, V. (2020). *Building a virtual maritime logistics cybersecurity training platform* (pp. 223-246). In Proceedings of the Hamburg International Conference of Logistics. Hamburg, Germany. https://doi.org/10.15480/882.3130

Rahman, R. (2023). *Cyber-attack threatens release of port of Lisbon data. Port Technology International*. Retrieved from https://www.porttechnology.org/news/cyber-attack-threatens-release-of-port-of-lisbon-data

Robinson, T. (2023). *Lockbit 3.0 claims credit for ransomware attack on Japanese port - security boulevard*. Retrieved from https://securityboulevard.com/2023/07/lockbit-3-0-claims-credit-for-ransomware-attack-on-japanese-port

Santamarta, R. (2015). *Maritime security: Hacking into a voyage data recorder (vdr).* Retrieved from https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr

Seong, K. T., Kim, G. H. (2019). Implementation of voyage data recording device using a digital forensics-based hash algorithm. *International Journal of Electrical and Computer Engineering, 9*, 5412-5419. https://doi.org/10.11591/ijece.v9i6.pp5412-5419

SHIP IP. (2024). *Maritime vulnerability and penetration testing*. Retrieved from https://shipip.com/maritime-vulnerability-and-penetration-testing

Sicard, F., Hotellier, E., & Francq, J. (2022). *An industrial control system physical testbed for naval defense cybersecurity research* (pp. 413-422). In Proceedings of the IEEE European Symposium on Security and Privacy Workshops. Genoa, Italy. https://doi.org/10.1109/EuroSPW55150.2022.00049

Silgado, D. M. (2018). *Cyber-attacks: A digital threat reality affecting the maritime industry*. Retrieved from https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations.

Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2023). Cybersecurity risk assessment of VDR. Journal of Navigation, 76(1), 20-37. https://doi.org/10.1017/S0373463322000595

Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). Risk sensitivity analysis of ais cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research, 142*, 103855. https://doi.org/10.1016/j.apor.2023.103855

Spivey, M. D. (2021). Vulnerability scanning. *Practical Hacking Techniques and Countermeasures, 2021*, 369-522. https://doi.org/10.1201/9781420013382-10

Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019a). Assessing ship cyber risks: A framework and case study of ecdis security. *WMU Journal of Maritime Affairs, 18*, 509-520. https://doi.org/10.1007/s13437-019-00183-x

Svilicic, B., Kristic, M., Zuskin, S., & Brcic, D. (2020a). Paperless ship navigation: Cyber se-curity weaknesses. *Journal of Transportation Security, 13*, 203-214. https://doi.org/10.1007/s12198-020-00222-2.

Svilicic, B., Rudan, I., Francic, V., & Doricic, M. (2019b). Shipboard ECDIS cyber security: Third-party component threats. *Pomorstvo, 33*(2), 176-180. https://doi.org/10.31217/p.33.2.7

Svilicic, B., Rudan, I., Francic, V. F., & Mohovic, D. M. (2020b). Towards a cyber secure shipboard radar. *Journal of Navigation, 73*(3), 547-558. https://doi.org/10.1017/S0373463319000808

Svilicic, B., Rudan, I., Jugovic, A. J., & Zec, D. (2019c). A study on cyber security threats in a shipboard integrated navigational system. *Journal of Marine Science and Engineering, 7*(10), 364. https://doi.org/10.3390/jmse7100364

Tabish, N., & Chaur-Luh, T. (2024). Maritime autonomous surface ships: A review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access, 12*, 17114-17136. https://doi.org/10.1109/ACCESS.2024.3357082

Tam, K., Forshaw, K., & Jones, K. (2019). *Cyber-ship: Developing next generation maritime cyber research capabilities* (pp. 1-10). In Proceedings of the International Conference on Marine Engineering and Technology. Oman. https://doi.org/10.24868/icmet.oman.2019.005

Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish A. V., Gimenez, P., Crichton, T., & Jones, K. (2021a). Case study of a cyber-physical attack affecting port and

ship operational safety. *Journal of Transportation Technologies, 12*(1), 1-27. https://doi.org/10.4236/jtts.2022.121001
Tam, K., & Jones, K. (2019). Macra: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs, 18*, 129-163. https://doi.org/10.1007/S13437-019-00162-2
Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Jornal of Cyber Policy, 3*(2), 147-164. https://doi.org/10.1080/23738871.2018.1513053
Tam, K., Moara-Nkwe, K., & Jones, K. (2021b). *A conceptual cyber-risk assessment of port infrastructure*. In Proceedings of the 2021 World of Shipping Portugal International Research Conference on Maritime Affairs, Portugal. Retrieved from https://api.semanticscholar.org/CorpusID:229406582
Tam, K., Moara-Nkwe, K., & Jones, K. D. (2021c). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research, 3*(1), 16-30. https://doi.org/10.33175/mtr.2021.241410
The Times of Israel. (2023). *Websites of Israeli port hacked; Sudanese group said to claim responsibility - the Times of Israel*. Retrieved from https://www.timesofisrael.com/websites-of-israeli-port-hacked-sudanese-group-said-to-claim-responsibility
UNCTAD. (2022). *Review of maritime transport 2022*. Retrieved from https://unctad.org/system/files/official-document/rmt2022_en.pdf
US Coast Guard. (2022). *2021 cyber trends and insights in the marine environment*. Retrieved from https://www.dco.uscg.mil/Portals/9/2021CyberTrendsInsightsMarineEnvironmentReport.pdf
US Coast Guard. (2024). *2023 cyber trends and insights in the marine environment*. Retrieved from https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf
Vineetha, H. A., Tam, K., & Jones, K. (2022). *Investigating the security and accessibility of voyage data recorder data using a usb attack*. Retrieved from https://www.researchgate.net/publication/365365607_Investigating_the_Security_and_Accessibility_of_Voyage_Data_Recorder_Data_using_a_USB_attack
Vineetha, H. A., Tam, K., & Jones, K. (2024). Bridgeinsight: An asset profiler for penetration testing in a heterogeneous maritime bridge environment. *Maritime Technology and Research, 6*(1), 266818. https://doi.org/10.33175/MTR.2024.266818
Walter, M. J., Barrett, A., & Tam, K. (2024). A red teaming framework for securing AI in maritime autonomous systems. *Applied Artificial Intelligence, 38*(1), 2395750.
Walter, M. J., Barrett, A., Walker, D. J., & Tam, K. (2023). Adversarial AI testcases for maritime autonomous systems. *AI, Computer Science and Robotics Technology, 2023*(2), 1-29. https://doi.org/10.5772/ACRT.15
Wolsing, K., Saillard, A., Bauer, J., Wagner, E., van Sloun, C., Fink, I. B., Schmidt, M., Henze, M., & Wehrle, K. (2022). *radarsec-lab*. Retrieved from https://doi.org/10.5281/zenodo.7188549
Yi, C. G., & Kim, Y. G. (2021). Security testing for naval ship combat system software. *IEEE Access, 9*, 66839-66851. https://doi.org/10.1109/ACCESS.2021.3076918
Yoo, Y., & Park, H. S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *Journal of Marine Science and Engineering, 9*(6), 565. https://doi.org/10.3390/jmse9060565
Yousaf, A., Amor, A., Kwa, P. T. H., Li, M., & Zhou, J. (2024). Cyber risk assessment of cyber-enabled autonomous cargo vessel. *International Journal of Critical Infrastructure Protection, 46*, 100695. https://doi.org/10.1016/j.ijcip.2024.100695
Zagan, R., Raicu, G., & Sabau, A. (2022). Studies and research regarding vulnerabilities of marine autonomous surface systems (mass) and remotely operated vessels (rovs) from point of view

of cybersecurity. *International Journal of Modern Manufacturing Technologies, XIV*, 2067-3604. https://doi.org/10.54684/ijmmt.2022.14.3.310